The Bateman-Horn constant for $x^3 + x + 1$

Timothy Foo
S080074@ntu.edu.sg

Abstract

We evaluate the Bateman-Horn constant for the polynomial $x^3 + x + 1$.

Conventions used here: $Q_1 = (\log x)^c$, $Q = x^{1-\epsilon}$, The Major Arcs are

$$\mathfrak{M} = \bigcup_{q \leq Q_1} \bigcup_{\substack{a=1 \\ (a,q)=1}}^{q} \left[\frac{a}{q} - \frac{1}{qQ}, \frac{a}{q} + \frac{1}{qQ} \right]. \tag{1}$$

For irreducible polynomials of the form $x^n + k$, the Bateman-Horn constant can be evaluated by the Hardy-Littlewood Circle Method via mimicking the method in [BZ]. The splitting fields of the polynomials $x^n + k$ which are irreducible form a class of extensions of number fields called Kummer extensions. Here, we try to evaluate the Bateman-Horn constant for $x^3 + x + 1$, a polynomial which is not of the form $x^n + k$. Facts about $x^3 + x + 1$, taken from [V], are the following: It has Galois group $G \simeq S_3$, its splitting field H is an unramified cubic extension of $\mathbb{Q}[\sqrt{-31}]$, and since $h(-31) = 3$, H is the Hilbert class field of $\mathbb{Q}[\sqrt{-31}]$. The Bateman-Horn constant is defined by

$$C(f) = \prod_p \left(\frac{p - n_p}{p - 1} \right)$$

where n_p is the number of solutions to the equation $f(n) \equiv 0 \bmod p$ in $\mathbb{Z}/p\mathbb{Z}$. For the polynomial $x^3 + x + 1$, we have that $n_p = 1, 3$ or 0, according to whether $\left(\frac{-31}{p}\right) = -1$, $\left(\frac{-31}{p}\right) = 1$ and p can be represented by the binary quadratic form $x^2 - xy + 8y^2$, or $\left(\frac{-31}{p}\right) = 1$ and p cannot be represented by the binary quadratic form $x^2 - xy + 8y^2$ respectively. This indicates that its Bateman-Horn constant should have the form

$$C(x^3 + x + 1) = \left(\frac{31 - 2}{31 - 1} \right) \prod_{\left(\frac{-31}{p}\right)=1}^{p} \left(\frac{p - n_p}{p - 1} \right).$$

We will mimick the method in [BZ] and make changes in the necessary places. In particular, the sum $S_1(\alpha)$ is unchanged and is defined as follows:

$$S_1(\alpha) = \sum_{m<z} \Lambda(m) e(\alpha m). \tag{2}$$

We have

$$S_1(\alpha) = T_1(\alpha) + E_1(\alpha) + o(x)$$

where

$$\alpha = \frac{a}{q} + \beta$$

with $|\beta| < \frac{1}{qQ}$.
Let

$$\tau(\chi) = \sum_{r \bmod q} \chi(r) e\left(\frac{r}{q}\right). \tag{3}$$

Then

$$T_1(\alpha) = \frac{\mu(q)}{\phi(q)} \sum_{m<z} e(\beta m)$$

and

$$\begin{aligned} E_1(\alpha) &= \frac{\mu(q)}{\phi(q)} \sum_{m \le z} (\Lambda(m) - 1) e(\beta m) \\ &+ \frac{1}{\varphi(q)} \sum_{\substack{r \bmod q \\ (r,q)=1}} \left(\sum_{\chi \neq \chi_0} \chi(ar) \tau(\bar{\chi}) \right) \sum_{\substack{m \equiv r \bmod q \\ m \le z}} \Lambda(m) e(\beta m) \\ &= \frac{\mu(q)}{\phi(q)} \sum_{m \le z} (\Lambda(m) - 1) e(\beta m) \\ &+ \frac{1}{\varphi(q)} \sum_{\chi \neq \chi_0} \tau(\bar{\chi}) \chi(a) \sum_{m<z} \chi(m) \Lambda(m) e(\beta m). \end{aligned}$$

But now we must define $S_2(\alpha)$ as follows:

$$S_2(\alpha) = \sum_{n \le x} e(-\alpha(n^3 + n)). \tag{4}$$

Then we have

$$\begin{aligned} S_2(\alpha) &= \sum_{n \le x} e\left(-\left(\frac{a}{q} + \beta\right)(n^3 + n) \right) \\ &= \sum_{d|q} \frac{1}{\varphi(q_1^*)\varphi(q^*)} \sum_{\chi_1 \bmod q_1^*, \chi_2 \bmod q^*} \chi_1(-ad^*) \chi_2(-a) \tau(\bar{\chi_1}) \tau(\bar{\chi_2}) \\ &\times \sum_{\substack{n \le x \\ (n,q)=d}} \chi_1(n^{*3}) \chi_2(n^*) e(-\beta(n^3 + n)), \end{aligned}$$

where

$$\begin{aligned} q^* &= \frac{q}{d}, \\ n^* &= \frac{n}{d}, \\ d^* &= \frac{d^2}{(d^2, q^*)}, \\ \text{and } q_1^* &= \frac{q^*}{(d^2, q^*)}. \end{aligned}$$

Later on, the $\mu(q)$ occuring in $T_1(\alpha)$ will restrict us to squarefree q, whence we have $q_1^* = q^* = q/d$ and $d^* = d^2$ Therefore, considering only squarefree q,

$$\begin{aligned} S_2(\alpha) &= \sum_{d|q} \frac{1}{\varphi(q^*)^2} \sum_{\chi_1, \chi_2 \bmod q^*} \chi_1(-ad^2)\chi_2(-a)\tau(\bar{\chi_1})\tau(\bar{\chi_2}) \\ &\times \sum_{\substack{n \le x \\ (n,q)=d}} \chi_1(n^{*3})\chi_2(n^*)e(-\beta(n^3+n)). \end{aligned}$$

So

$$\begin{aligned} S_2(\alpha) &= \sum_{d|q} \frac{1}{\varphi(q^*)^2} \sum_{\substack{\chi_1, \chi_2 \bmod q^* \\ \chi_1^3\chi_2 = \chi_0}} \chi_1(-ad^2)\chi_2(-a)\tau(\bar{\chi_1})\tau(\bar{\chi_2}) \sum_{\substack{n \le x \\ (n,q)=d}} e(-\beta(n^3+n)) \\ &+ \sum_{d|q} \frac{1}{\varphi(q^*)^2} \sum_{\substack{\chi_1, \chi_2 \bmod q^* \\ \chi_1^3\chi_2 \neq \chi_0}} \chi_1(-ad^2)\chi_2(-a)\tau(\bar{\chi_1})\tau(\bar{\chi_2}) \sum_{\substack{n \le x \\ (n,q)=d}} \chi_1(n^{*3})\chi_2(n^*)e(-\beta(n^3+n)) \\ &= T_2(\alpha) + E_2(\alpha), \text{ say,} \end{aligned}$$

Now

$$\begin{aligned} &\sum_{\substack{\chi_1, \chi_2 \bmod q^* \\ \chi_1^3\chi_2 = \chi_0}} \chi_1(-ad^2)\chi_2(-a)\tau(\bar{\chi_1})\tau(\bar{\chi_2}) \\ &= \sum_{\chi \bmod q^*} \chi(a^{-2}d^2)\tau(\bar{\chi})\tau(\chi^3) \end{aligned}$$

where a^{-2} means a inverse squared in $(\mathbb{Z}/(q^*)\mathbb{Z})^*$.
Therefore, we have

$$T_2(\alpha) = \sum_{d|q} \frac{1}{\varphi(q^*)^2} \sum_{\chi \bmod q^*} \chi(a^{-2}d^2)\tau(\bar{\chi})\tau(\chi^3) \sum_{\substack{n \le x \\ (n,q)=d}} e(-\beta(n^3+n)). \quad (5)$$

The main term will be given by the following:

$$\int_{\mathfrak{M}} T_1(\alpha)T_2(\alpha)e(-\alpha)d\alpha \tag{6}$$
$$= \sum_{q\le Q_1}\frac{\mu(q)}{\varphi(q)}\sum_{\substack{a \bmod q\\(a,q)=1}} e\left(\frac{-a}{q}\right)\sum_{d|q}\frac{1}{\varphi(q^*)^2}\sum_{\chi \bmod q^*}\chi(a^{-2}d^2)\tau(\bar{\chi})\tau(\chi^3)\int_{|\beta|<\frac{1}{qQ}}\Pi_{q,d}(\beta)d\beta$$

where

$$\Pi_{q,d}(\beta)=\sum_{m\le z}e(\beta m)\sum_{\substack{n\le x\\(n,q)=d}}e(-\beta(n^3+n+1)). \tag{7}$$

We approximate

$$\int_{|\beta|<\frac{1}{qQ}}\Pi_{q,d}(\beta)d\beta$$

by

$$\int_0^1\sum_{m\le z}e(\beta m)\sum_{\substack{n\le x\\(n,q)=d}}e(-\beta(n^3+n+1))d\beta$$
$$+\quad O\left(\int_{1/qQ}^{1/2}\frac{1}{\beta}\left|\sum_{\substack{n\le x\\(n,q)=d}}e(-\beta(n^3+n+1))\right|d\beta\right).$$

and the O-term in the above is, by Cauchy's inequality and Parseval's identity,

$$\ll\left(\int_{1/qQ}^{1/2}\frac{1}{\beta^2}d\beta\right)^{\frac{1}{2}}\left(\int_0^1\left|\sum_{\substack{n\le x\\(n,q)=d}}e(-\beta(n^3+n+1))\right|^2d\beta\right)^{\frac{1}{2}}\ll(\frac{qQx}{d})^{\frac{1}{2}}. \tag{8}$$

Furthermore,

$$\int_0^1\sum_{m\le z}e(\beta m)\sum_{\substack{n\le x\\(n,q)=d}}e(-\beta(n^3+n+1))d\beta=\sum_{\substack{n\le x\\(n,q)=d}}1=\frac{\varphi(q/d)x}{q}+O(\varphi(q/d)). \tag{9}$$

Therefore,

$$\int_{\mathfrak{M}} T_1(\alpha)T_2(\alpha)e(-\alpha)d\alpha \tag{10}$$
$$= \sum_{q\le Q_1}\frac{\mu(q)}{\varphi(q)}\sum_{\substack{a \bmod q\\(a,q)=1}} e\left(\frac{-a}{q}\right)\sum_{d|q}\frac{1}{\varphi(q^*)^2}$$
$$\times\sum_{\chi \bmod q^*}\chi(a^{-2}d^2)\tau(\bar{\chi})\tau(\chi^3)\left(\frac{\varphi(q/d)}{q}x+O\left(\left(\frac{qQx}{d}\right)^{\frac{1}{2}}\right)\right)$$

This yields

$$x\sum_{q=1}^{\infty}\frac{\mu(q)}{\varphi(q)q}\sum_{\substack{a \bmod q\\(a,q)=1}} e\left(\frac{-a}{q}\right)\sum_{d|q}\frac{1}{\varphi(q/d)}\sum_{\chi \bmod q^*}\chi(a^{-2}d^2)\tau(\bar{\chi})\tau(\chi^3)$$

$+$ error terms.

Now, comparing the singular series obtained here with the Bateman-Horn constant, we obtain the following formula for n_p, the number of solutions to the equation $n^3+n+1\equiv 0 \bmod p$ in $\mathbb{Z}/p\mathbb{Z}$:

$$n_p - 1 = \frac{1}{p}\sum_{\substack{a \bmod p\\(a,p)=1}} e\left(\frac{-a}{p}\right)\sum_{d|p}\frac{1}{\varphi(p/d)}\sum_{\chi \bmod (p/d)}\chi(a^{-2}d^2)\tau(\bar{\chi})\tau(\chi^3). \quad (11)$$

It seems that irreducible polynomials of the form x^n+k which generate Kummer extensions are the easiest ones to handle when evaluating n_p via this method. For these, the right hand side of the above collapses into a sum over Dirichlet characters which reflects the arithmetic of the Kummer extension - the Dirichlet characters are actually Hecke characters on the narrow ray class group of a certain conductor which is canonically isomorphic, by Artin Reciprocity, to the Galois group of the ray class field E of $F=\mathbb{Q}[e^{\frac{2\pi i}{n}}]$ over F. (E contains $F[k^{\frac{1}{n}}]$ as a subfield.) For x^3+x+1 already we have to sum a product of Gauss sums over all characters modulo p/d (as in (5) and (11))as opposed to only those of a given order as in the case of x^n+k. As the situation becomes more complicated, it is unclear how the right hand side of the above reflects the arithmetic of the field.

References

[BZ] S. Baier and L. Zhao, Primes in Quadratic Progressions on Average, Math. Ann., Vol 338, 2007, No. 4, 963–982

[V] F.R. Villegas, Experimental Number Theory, Oxford University Press, 2007